Q&A Document for Washington Post Going Dark Interview

Answers vetted and approved by OTD, OGC

1. **Has the Going Dark problem gotten worse for law enforcement over the past year? How?**

The impediments faced by law enforcement have been getting worse for quite some time. As technology continues to advance, new services introduced, and the number of providers increase, law enforcement faces an increasing number of diverse challenges.

Many of the newest communications services are developed and deployed without consideration of law enforcement's lawful intercept needs. There is no requirement for many companies to do so. As you know, CALEA applies to traditional telecommunications carriers, providers of interconnected Voice over Internet Protocol (VoIP) services, and providers of broadband access services. Traditional providers have been covered since 1994 and VoIP and broadband have been covered since a 2005 FCC ruling. That's a long time ago in terms of the industry.

Over the last year, many providers have used what has been reported in the media about bulk collection to keep law enforcement at a distance even though law enforcement has neither the authorities nor comparable capabilities to those reported. Law enforcement is dependent on direct provider assistance to conduct court ordered electronic surveillance.

2. **Has the FBI experienced any reduced cooperation from communication providers as a result of the disclosures attributed to Edward Snowden?**

Yes. There is a growing concern within the industry that the perception of assisting law enforcement reflects negatively on communications providers. Law enforcement is being swept into the broad generalization that providing *any* assistance to the government is tantamount to disregarding their user's rights to privacy. In addition to providing evidence of crimes, that assistance does provide to law enforcement the necessary information to rule out subjects from any further investigation.

There has also been a loss of recognition that law enforcement must get the prior authorization of a court to request a communications provider to assist it in conducting electronic surveillance and that law enforcement must abide by the rigorous constructs of law when applying for a court order.

As a result, what is happening is that capabilities are not being developed to address the real day-to-day needs of law enforcement when a court grants that lawful authority.

3. **Why does law enforcement believe companies should be forced to build in backdoors when designing services? Don't backdoors pose a security risk for companies?**

That's a common misperception of what law enforcement needs and what law enforcement is requesting. Law enforcement is not asking for unfettered access into any provider's network. Let's talk about the CALEA paradigm – the industry develops a technical standard through its

normal specification processes; a provider controls the technical solution resident in it network; it ensures its network is capable of isolating only the target identified in the court order; it activates the interception; and it disables the interception with the order expires. Law enforcement is the recipient of the information collected by the provider. This is a "front door" approach – where law enforcement first gains the lawful authority and then serves the provider with the court order that directs the provider to conduct the intercept. That's the corollary we're looking for with more modern communications services.

It's important to stress that an open, transparent process for identifying technical capabilities benefits everyone. First, the public can be assured that the capabilities are commensurate with the already existing authorities granted to law enforcement by statute. Second, the industry understands its responsibilities and all providers are held to the same standard (i.e., the level playing field). Third, law enforcement can be confident that it will receive what it needs and is authorized by law to collect, regardless of the specific service provider.

Law enforcement believes that providers can minimize any risks by developing intercept solutions during the service's design phase. Such solutions are likely to be better, smarter, cheaper, and more secure than solutions that are retrofitted to existing products. There was similar apprehension during the initial stages of discussions about CALEA – that there would be an increased security risk in having technical solutions resident in carriers' networks. That prediction has not come to pass.

4. The FBI has launched the NDCAC. Is it working as expected? Can I learn more about the NDCAC?

Yes. The NDCAC was designed as a hub for technical knowledge management that facilitates the sharing of solutions and know-how among law enforcement agencies, and strengthens law enforcement's relationships with the communications industry. The NDCAC leverages / shares law enforcement's collective technical knowledge and resources on issues involving real-time and stored communications to address challenges posed by advanced communications services and technologies. But, it can't solve all of law enforcement's problems – it allows a certain measure of self-help within the community. The entire community still necessarily relies on industry's assistance.

It is important to note that the NDCAC does not conduct research and development, is not responsible for the execution of any electronic surveillance court orders, and does not have any direct operational or investigative role in investigations. Rather, the NDCAC provides technical knowledge and referrals in response to requests for assistance from any member of the law enforcement community. The NDCAC also leverages the training capabilities of certain law enforcement agencies to benefit a larger portion of the community.

More information is available on the website: http://www.ndcac.cjis.gov

5. It has been reported the government receives a daily dump...screen shots from companies...why is this not good enough?

In some cases subject to legal process, it may be enough that law enforcement receives a daily

report of the lawfully authorized information. But in many instances, the information is incomplete or not provided in a timely manner to support every type of investigative requirement, especially when dealing with crimes in motion (e.g., kidnapping, extortion, drug trafficking). Also, not every company has the capability. Further, there is significant disparity in what companies offering similar services can provide to law enforcement – there is simply not a lot of consistency across the board.

There is also an issue with law enforcement receiving "screen shots" in that they are typically no more than a picture file. Law enforcement needs the information in a format that is readily usable for effective analysis.

Law enforcement believes a mandate would necessitate a vitally important discussion about what providers must furnish to law enforcement in response to a court order. Importantly, that discussion would result in uniformity in the information law enforcement can expect from providers and what companies can expect to provide.

6. Confirmation or comment on companies outright refusing to court order? How many times do you take it to court?

There are a number of ways companies can thwart law enforcement's attempts – refusing to implement a court order or delaying that implementation can irreparably set back an investigation. Law enforcement understands that there may be instances where it is technically not feasible for a company to provide assistance, but absent some insight into how a company provides service, it is impractical for law enforcement to understand the root cause of some instances where a company refuses to comply with a court order.

The primary court-based recourse available to law enforcement is to pursue an order to show cause. In essence, a court would require a company to explain why it cannot meet the requirements of the court's order to assist in the implementation of an interception. The decision to pursue show cause orders is very case-specific and can in some instances spur a company to be more responsive. However, this process often extends well beyond the time limitations of the original court order and historically has not proven to be an effective use of already scarce law enforcement resources.

7. Has the problem of encryption gotten worse since Snowden, with more companies advertising encryption services? How is the FBI dealing with enhanced encryption?

Yes. In the rush to address bulk collection, law enforcement's needs are being overlooked.

A number of the country's largest providers have been very openly vocal about their concerns regarding surveillance and have published an open letter to the President and members of Congress. Law enforcement has no issue with these companies' commitment to "*keeping users' data secure — deploying the latest encryption technology to prevent unauthorized surveillance on our networks and by pushing back on government requests to ensure that they are legal and reasonable in scope.*"

What is missing is a vigorous commitment to assist law enforcement when electronic

surveillance is authorized – that element seems to have been lost in this discussion. It is vitally important to distinguish between law enforcement's use of lawfully authorized electronic surveillance and "bulk collection."

What is needed now is an open and frank dialogue about the responsibilities of industry to assist law enforcement. The statutory authorities are already in place and law enforcement isn't seeking additional authority.

Industry and law enforcement need to move forward and develop a framework under which both sides participate in striking an appropriate balance among the public's privacy interests, the industry's goals of competition and innovation, and the needs of law enforcement.

8. Numbers and case examples to demonstrate the problem (for both criminal and national security).

Provided separately

Follow-up Q&S for Washington Post Going Dark Interview

Answers vetted and approved by OTD, OGC

1. **Here's the dilemma as the government sees it. Wiretap law requires a company or individual to provide "technical assistance" to an official with a valid electronic surveillance order. But most Internet-related companies are not required by law to make sure that their systems are wiretap-ready. And the phrase "technical assistance" is vague, permitting differences of interpretation. Correct?**

Yes. The dilemma can best be characterized as follows. The impediments faced by law enforcement have been getting worse for quite some time. As technology continues to advance, new services are introduced, and the number of providers increase, law enforcement faces an increasing number of diverse challenges. Many of the newest communications services are developed and deployed without consideration of law enforcement's "lawful intercept" needs (i.e., legally authorized electronic surveillance). CALEA applies to traditional telecommunications carriers, providers of interconnected Voice over Internet Protocol (VoIP) services, and providers of broadband access services. "Traditional" providers have been covered under CALEA since 1994, and VoIP and broadband have been covered since a 2005 FCC ruling. That is a long time ago in terms of this industry and CALEA does not impact a significant number of communications service providers in today's marketplace.

It is also important to note that the "technical assistance" clause in federal wiretap law is often insufficient. The assistance furnished by some providers simply does not provide law enforcement with the information it requested and which it needs to fully understand or acquire the relevant communications. It is more than a difference of interpretation in that, without more specific guidance as to what constitutes "technical assistance," a provider may do all that it can and still not be able to provide law enforcement the information it needs to do its job.

As a practical matter, a CALEA compliant provider who has a built an intercept capability into its architecture will most likely be able to assist law enforcement immediately, whereas a provider that has no solution and attempts to render "technical assistance" likely will not. In most instances, providers attempting to render assistance must divert resources to react to an immediate situation, such as a hostage-taking or kidnapping scenario, where time is of the essence. Despite their best efforts, critical information will be lost due to the delay.

2. **Wanted to confirm that Amy was saying: Anything short of real time interception is not fully complying "because we didn't get all the information we needed or because it wasn't provided consistently."**

In many instances, information provided in response to intercept orders is incomplete or not provided in a timely manner to support every type of investigative requirement, especially when dealing with crimes in motion (e.g., kidnapping, extortion, drug trafficking). Also, not every company has an intercept capability and there is significant disparity in what companies offering similar services can provide to law enforcement. There is simply a lack of consistency across the

industry. The lack of capability and lack of consistency negatively impact law enforcement's ability to fully understand the extent of a criminal's activities, identification of co-conspirators, and location of victims.

3. **On DRIP: It looks like the British parliament is going to pass the law. It will not only ensure that U.K. companies store customer data for the government but it gives the government the right to require non-U.K. companies outside the country to build wiretap capabilities. My understanding is that the FBI several years ago floated draft legislation that included an analogous provision—to require non US companies outside the US to build wiretap capabilities if directed, but the proposal died. Please let me know if that is not correct.**

It is premature to comment on how the UK legislation will impact United States law enforcement's ability to effect court orders, however, it does reflect the fact that the UK is facing a similarly daunting challenge in conducting electronic surveillance.

4. **Also, I am told that there has never been a fine issued under either CALEA or the 2518 provision of the Wiretap Act.**

It is true that fines have not been issued under the CALEA enforcement provisions set forth in Title 18 U.S.C. Section 2522 which, in turn, incorporate the provisions of Section 108 of CALEA. As written, the enforcement provisions are cumbersome and the pursuit of enforcement can be a lengthy, complicated, and resource-intensive process. In many cases, the investigation which identified the capability gap would be closed long before any action would be taken. However, it is not correct to imply that the enforcement provision of the law cannot have any effect. The enforcement provision allows law enforcement to raise non-compliance issues to the attention of a company's senior management and/or general counsel and work toward a common understanding of the company's obligations. Law enforcement and prosecutors are more interested in ensuring companies have the appropriate capabilities at their disposal when served with a court order than pursuing fines or penalties through prolonged litigation of the underlying issues, but this option remains viable, if needed.

5. **Still would like to know your response to experts who say that building in a wiretap solution builds in insecurity into the system.**

Developing intercept solutions during the service's design phase allows providers to minimize risk from the outset. Such solutions are likely to be better, smarter, cheaper, and more secure than solutions that are retrofitted to existing products. There was similar apprehension during the initial stages of discussions about CALEA, i.e. that there would be an increased security risk in having technical solutions resident in carriers' networks. That prediction has not come to pass. In fact, as intended when CALEA was passed, individuals' privacy interests are better protected when a company has an intercept solution in place that allows them to isolate and provide to law enforcement only those communications of the individuals who are subject to the court order.

An open, transparent process for identifying technical lawful intercept capabilities benefits everyone. Privacy advocates and the public can be assured the capabilities are commensurate with authorities that already exist and are granted to law enforcement by statute. In other words, law enforcement is not asking for additional authorities, but rather just the ability to use the authorities we already have. Under this construct, industry will clearly understand its responsibilities and all providers will be held to the same standard (i.e., the level playing field). Moreover, law enforcement can be assured it will receive what it is authorized to collect, regardless of service provider.

6. Still interested in the rough number of companies/apps that the FBI knows will not provide RT data.

There are hundreds of communication service providers which meet this definition. The FBI has experienced numerous situations when a communication service provider cannot or will not provide real time data. In some instances, the FBI leverages its Engineering Research Facility to help develop a solution, working cooperatively with the company. In other situations, depending on the nature of the service, it may be feasible to gain alternative access to another service provider and isolate the communications of the suspect. There have been instances where those avenues are determined to not be feasible and the FBI does not pursue obtaining a court order. The number of such communication service providers that offer new services which do not have an electronic surveillance capability continues to grow as technology continues to evolve.